An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One

L Swales*

P·E·R
Pioneer in peer-reviewed, open access online law publications

Author

Lee Swales

Affiliation

University of KwaZulu-Natal
South Africa

Email swalesl@ukzn.ac.za

Date of submission

11 July 2017

Date published

19 March 2018

Editor Dr A Gildenhuys

How to cite this article

Swales L "An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One"*PER / PELJ* 2018(21) - DOI http://dx.doi.org/10.17159/1727-3781/2018/v21i0a2916

DOI
http://dx.doi.org/10.17159/1727-3781/2018/v21i0a2916

Abstract

The purpose of this two-part article is to examine the regulatory environment governing hearsay electronic evidence in South Africa – with a view to providing clear, practical suggestions for regulatory reform in the context of the South African Law Reform Commission's most recent Discussion Paper on electronic evidence.

Technology has become an indispensable part of modern life. In particular, the Internet has facilitated new forms of business enterprise, and shifted basic communication norms. From a legal perspective, technology has presented several novel challenges for courts and legal practitioners to deal with – one of these key challenges relates to electronic evidence and in particular the application of the hearsay rules to the digital environment.

The South African Law Reform Commission has identified the application of the hearsay rule as one of the core concerns with regard to electronic evidence, and certain academic analysis has revealed inefficiency in the current legal position which may involve multiple sources of law. Moreover, the Law Society of South Africa has stated that there is some confusion amongst members of the profession in relation to hearsay as it applies to electronic evidence.

With the pervasive and burgeoning nature of technology, and with the Internet in mind, it is natural to assume that electronic evidence will be relevant in most forms of legal proceedings in future, and hearsay electronic evidence in particular will play an increasingly important role in years to come.

Consequently, part one of this article will consider the key definitional concept in relation to electronic evidence – data messages - and examine whether the definition should be revised. In addition, part one of this article will answer two further critical questions posed by the South African Law Reform Commission in relation to data messages and hearsay evidence, namely: should a data message constitute hearsay? And, how should one distinguish between documentary evidence and real evidence in the context of data messages?

Keywords

Electronic evidence; data messages; *ECT Act*; law of evidence; South African Law Reform Commission; technology and law.

.....

1 Introduction

Technology has become an indispensable part of modern life.[1] In particular, the Internet has facilitated new forms of business enterprise and shifted basic communication norms.[2] With the proliferation[3] of technology involved in day-to-day life, the only reasonable inference one can draw is that electronic evidence will play an increasingly important role in most forms of legal proceedings – both now and in the future.

The pervasive and burgeoning nature of advancing technology has forced change to the administration of justice, and presented several novel challenges for courts and legal practitioners to deal with.[4] According to the South African Law Reform Commission (SALRC), in this context: "the application of the hearsay rule is one of the core concerns with regard to electronic evidence".[5]

Certain academic analysis has revealed inefficiency[6] with the current legal position (which may involve multiple sources of law). Moreover, the Law Society of South Africa has stated that, in relation to hearsay electronic evidence and related principles, there is some confusion amongst members of the profession.[7]

---

* Lee Swales. LLB (UKZN) LLM (Wits). Lecturer, School of Law, University of KwaZulu-Natal and Consultant Attorney Thomson Wilks Inc. E-mail: swalesl@ukzn.ac.za. A revised version of this paper was presented at a conference of the South African Association of Intellectual Property Law and Information Technology Law Teachers and Researchers hosted by Stellenbosch University on 21-22 June 2017. This paper forms part of an ongoing PhD study.

1 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 437; Papadopoulos and Snail *Cyberlaw@SA III* 1; Van der Merwe *et al Information and Communications Technology Law* 1.

2 *Delsheray Trust v ABSA Bank Limited* 2014 JOL 32417 (WCC) para 18 where the court noted, "modern technological developments have brought about a revolution in the way that information, including legal information, is captured and disseminated"; *Heroldt v Wills* 2013 2 SA 530 (GSJ) para 8 where Willis J stated, "the pace of the march of technological progress has quickened to the extent that the social changes that result therefrom require high levels of skill".

3 De Villiers (2) 2010 *TSAR* 723.

4 Although not exhaustive, the primary challenges are: the ease of manipulation of electronic evidence, rapidly evolving technology, the fragility of the media, dependency on certain specific hardware and/or software, and the fact that data on networked environments is regarded as dynamic and volatile. For a further discussion of these issues, see SALRC *Issue Paper 27* 7-15; De Villiers (1) 2010 *TSAR* 558; Watney 2009 *JILT* 3-4.

5 SALRC *Discussion Paper 131* 13.

6 SALRC *Discussion Paper 131* 66.

7 LSSA 2015 https://tinyurl.com/m9vght3.

Consequently, in order to provide clear and practical suggestions, this two-part article will review the applicable regulatory environment governing hearsay electronic evidence in South Africa,[8] and conclude with suggestions for law reform in the context of recommendations put forward by the SALRC (while also considering selected foreign jurisdictions – those of the United Kingdom, Canada and the United States, where electronic evidence has had more time to mature and develop).[9]

Part one of this article will consider the key definitional concept in relation to electronic evidence – data messages - and examine whether the definition should be revised.[10] In addition, part-one of this article will answer two further critical questions posed by the SALRC in relation to data messages and hearsay evidence, namely: should a data message constitute hearsay?[11] And, how should one distinguish between documentary evidence and real evidence in the context of data messages?[12]

2 Data messages

Computer- or machine-related evidence[13] is often referred to as electronic[14] evidence, digital evidence,[15] ESI evidence[16] (electronically stored information), computer evidence,[17] or ICT[18] evidence. None of these terms exists in South African statute. Instead, the term data message[19] is used.[20] South Africa drew this definition from the United Nations Commission on

8 Hofman and de Jager "South Africa" 761-796.

9 SALRC *Discussion Paper 131* 83-88.

10 SALRC *Discussion Paper 131* 52-55 where Issue 3 is framed as: should the definition of data message be revised?

11 SALRC *Discussion Paper 131* 62-67 where part of issue 6 is framed as: should a data message constitute hearsay within the meaning of section 3 of the Law of Evidence Amendment Act?

12 SALRC *Discussion Paper 131* 68-70 where part of issue 7 is framed as: should there be distinction between mechanically produced evidence without the intervention of the human mind and mechanically produced evidence with the intervention of the human mind?

13 Theophilopoulos 2015 *TSAR* 462-463 where the admissibility requirements for electronic documents are discussed.

14 Hofman and de Jager "South Africa" 761-796; Papadopoulos and Snail *Cyberlaw@SA III* 315.

15 Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 410.

16 Papadopoulos and Snail *Cyberlaw@SA III* 315.

17 The term used by van Zyl J in *S v Ndiki* 2007 2 ALL SA 185 (Ck) para 4.

18 Van der Merwe *et al Information and Communications Technology Law* 114-115.

19 SALRC *Discussion Paper 131* 2- 45; Zeffertt and Paizes *South African Law of Evidence* 843-847.

20 More broadly, the term "data" is used, and is defined in the *Electronic Communications and Transactions Act* 25 of 2002 as "electronic representation of information of any form"; Zeffertt and Paizes *South African Law of Evidence* 843.

International Trade Law (UNCITRAL) *Model Law on Electronic Commerce*, 1996 (*Model Law*, 1996).[21]

The first introduction[22] of the term data message[23] to South African law was on 30 August 2002 with the promulgation of the *Electronic Communications and Transactions Act* (the *ECT Act*).[24]

Interestingly, the promulgation of the proposed *Cybercrimes and Cybersecurity Bill*[25] in its current form will lead to the term data message having conflicting definitions. The current definition in the *ECT Act* reads as follows:

> 'data message' means data generated, sent, received or stored by electronic means and includes-
>
> (a) voice, where the voice is used in an automated transaction; and
>
> (b) a stored record.

The *Cybercrimes and Cybersecurity Bill*[26] defines the term as:

> 'data message' means data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form.

According to section 61 of the *Cybercrimes and Cybersecurity Bill*,[27] the definition of data message[28] contained within the *ECT Act* is not due to be

---

21 UN 1996 http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf; SALRC *Discussion Paper 131* 27-45; UNCITRAL 2017 http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html, where the Secretariat lists member states that comply with the *United Nations Commission on International Trade Law Model Law on Electronic Commerce* (1996) (hereafter *Model Law*, 1996). There are 67 States in a total of 143 jurisdictions that have adopted it. South Africa is largely compliant: "except for the provisions on certification and electronic signatures".

22 The *Electronic Communications and Transactions Act* 25 of 2002 followed the *Computer Evidence Act* 57 of 1983, which did not attempt to define electronic evidence – rather, it defined "information" as "any information expressed in or conveyed by letters, figures, characters, symbols, marks, perforations, patterns, pictures, diagrams, sounds or any other visible, audible or perceptible signals".

23 SALRC *Issue Paper 27* 31-33; SALRC *Discussion Paper 131* paras 52-55.

24 *Electronic Communications and Transactions Act* 25 of 2002 (hereafter ECT Act).

25 *Cybercrimes and Cybersecurity Bill* B6-2017.

26 The *Draft Cybercrimes and Cybersecurity Bill*, 2015 released for public comment (Gen N 878 in GG 39161 of 2 September 2015) used the same definition of data message as that now contained in the current *Cybercrimes and Cybersecurity Bill* B6-2017.

27 Section 61 *Cybercrimes and Cybersecurity Bill* B6-2017 (read together with the appropriate Schedule) does not list the definition of data message in the ECT Act on the list of the repeal of laws.

28 The *Draft Electronic Communications and Transactions Amendment Bill* 2012 (GN R888 in GG 35821of 26 October 2012), which proposed a further definition for data

repealed or amended. Although this is a minor oversight and of little practical effect, it should be corrected as soon as possible. That notwithstanding, the current definition of data message is not entirely satisfactory (whether in the *ECT Act* or the *Cybercrimes and Cybersecurity Bill*). It would benefit from an amendment along the following lines:

> 'Data message' means information generated, sent, received or stored by electronic means.

The definition[29] above should survive short- to medium-term technological development, and is concise and detailed enough without including superfluous terms, or including conditions that do not apply to traditional evidence.[30] It is also consistent with the proposals put forward by the SALRC[31] where it recommends that:

> There is clearly concern around the inclusion of the term - *voice, where the voice is used in an automated transaction* - in the definition of data message, and there do not appear to be compelling reasons to retain the term in the definition. The SALRC therefore proposes that the term be deleted or amended.

3 Hearsay electronic evidence: overview and context

The South African law of evidence is not codified in one single statute.[32] The *Constitution*,[33] a variety of statutes,[34] the common law,[35] and applicable case law must be considered to form a view on whether potential evidence is admissible, and if it is admissible, a view on the weight it should be accorded. In general, South Africa takes an exclusionary[36] approach to

---

messages, appears to have been withdrawn, which is a positive development – the definition was verbose and unnecessarily complicated.

29 See further the discussion of law reform proposals in the context of electronic evidence in Swales 2018 *PELJ* 17-25.

30 For a detailed discussion on "data message" and this issue in general, see SALRC *Discussion Paper 131* 13, 52-55.

31 SALRC *Discussion Paper 131* 52-55. It should be noted that the SALRC recommendations were made before any version of the *Cybercrimes and Cybersecurity Bill* was available for comment.

32 Bellengere *et al Law of Evidence* 4; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 24-31; De Villiers (1) 2010 *TSAR* 559.

33 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 27.

34 *Civil Proceedings Evidence Act* 25 of 1965; *Criminal Procedure Act* 51 of 1977; *Law of Evidence Amendment Act* 45 of 1988; ECT Act; and where applicable, *Constitution of the Republic of South Africa*, 1996.

35 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 26-27.

36 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 438; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 411; Papadopoulos and Snail *Cyberlaw@SA III* 317; Van der Merwe *et al Information and Communications Technology Law* 107; Hofman and De Jager "South Africa" 761; Watney 2009 *JILT* 5-11.

evidence in civil and criminal proceedings - this position mimics the English common law.[37]

Evidence will be considered admissible only if it is relevant to a fact at issue,[38] and even if relevant, the evidence will be admissible only if it is not excluded by a common law or statutory rule precluding the admissibility of a certain type[39] of evidence, or precluding the admissibility of evidence obtained in a certain manner.[40]

Any potential evidence that a party to civil or criminal proceedings wishes to admit to court will typically be classified under one or more of three headings: as an object (real evidence),[41] as a document (documentary evidence),[42] or evidence from a witness (oral evidence).[43]

South African courts are not yet equipped to deal with the variety of computer systems and programmes that produce data messages. Therefore, for practical reasons a data message is normally presented as a print-out when tendering the information as evidence.[44]

The key questions that arise are as follows: is a data message hearsay within the meaning of the *Law of Evidence Amendment Act*?[45] Moreover, if a data message is hearsay within the meaning of the *Law of Evidence*

37 *S v Ndiki* 2008 2 SACR 252 (Ck) para 21 where the common law position with regard to evidence is stated as follows: "evidence tending to prove or disprove an allegation which is in issue is admissible unless a specific ground for exclusion operates." Also see *R v Trupedo* 1920 AD 58 62; *R v Katz* 1946 AD 71 78; Hofman and De Jager "South Africa" 761; Papadopoulos and Snail *Cyberlaw@SA III* 316.

38 *R v Trupedo* 1920 AD 58 62; *S v Ndiki* 2008 2 SACR 252 (Ck) para 21.

39 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 287-304; Zeffertt and Paizes *South African Law of Evidence* 385-441; Bellengere *et al Law of Evidence* 234-245.

40 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 198-283; Zeffertt and Paizes *South African Law of Evidence* 721-736; *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 14.

41 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 421-430; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 395-402; Bellengere *et al Law of Evidence* 64-69; Zeffertt, Paizes and Skeen *South African Law of Evidence* 703-712.

42 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 431-436; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 404-409; Bellengere *et al Law of Evidence* 59-63; Zeffertt, Paizes and Skeen *South African Law of Evidence* 685-695.

43 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 387-420; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 361-394; Bellengere *et al Law of Evidence* 51-58.

44 *S v Ndiki* 2008 2 SACR 252 (Ck); *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a La Enterprises* 2011 4 SA 577 (GSJ). This observation also accords with my own personal experience in practice.

45 These questions are based on SALRC *Discussion Paper 131* 52-71.

Amendment Act, then to what extent, if any, does the *ECT Act* "liberate"[46] the data message from the exclusionary hearsay rule? Further, and irrespective of whether a data message can be hearsay, how does one consistently determine whether a data message is documentary evidence or real evidence?[47]

Increasingly, parties to criminal and/or civil proceedings rely on some form of data messages as evidence, and the rules relating to hearsay are often at issue. It is not always cost-effective or reasonable to have every person testify, and the precise classification of a data message, together with its statutory exceptions, becomes increasingly important in modern legal proceedings.

4 Development of the legal position regulating hearsay electronic evidence

The promulgation of the *Law of Evidence Amendment Act*[48] took place in October 1988. It rendered the common law definition of hearsay[49] obsolete.[50] Section 3 (which deals with hearsay evidence) reads as follows:

> 3(1) Subject to the provisions of any other law, hearsay evidence shall not be admitted as evidence at criminal or civil proceedings, unless-
>
> (a) each party against whom the evidence is to be adduced agrees to the admission thereof as evidence at such proceedings;
>
> (b) the person upon whose credibility the probative value of such evidence depends, himself testifies at such proceedings; or
>
> (c) the court, having regard to-

46 Zeffertt and Paizes *South African Law of Evidence* 432.

47 *S v Ndiki* 2008 2 SACR 252 (Ck); *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a La Enterprises* 2011 4 SA 577 (GSJ); *Ex parte Rosch* 1998 1 All SA 319 (W); *S v Mashiyi* 2002 2 SACR 387 (Tk); *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W); *S v Brown* 2015 ZAWCHC 128 (17 August 2015). Also see Zeffertt and Paizes *South African Law of Evidence* 431-436; Hofman and De Jager "South Africa" 776-780; Theophilopoulos 2015 *TSAR* 464 (in particular note 9), 474 (in particular note 31); Fourie *Using Social Media as Evidence* 8-20.

48 *Law of Evidence Amendment Act* 45 of 1988.

49 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 287-304; Zeffertt and Paizes *South African Law of Evidence* 385-443.

50 *S v Ndiki* 2008 2 SACR 252 (Ck) para 31; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 269; Bellengere *et al Law of Evidence* 293-294; Zeffertt, Paizes and Skeen *South African Law of Evidence* 364-402; Zeffertt and Paizes *South African Law of Evidence* 389-416.

(i) the nature of the proceedings;

(ii) the nature of the evidence;

(iii) the purpose for which the evidence is tendered;

(iv) the probative value of the evidence;

(v) the reason why the evidence is not given by the person upon whose credibility the probative value of such evidence depends;

(vi) any prejudice to a party which the admission of such evidence might entail; and

(vii) any other factor which should in the opinion of the court be taken into account, is of the opinion that such evidence should be admitted in the interests of justice.

Importantly, section 3(4) defines hearsay as:

> evidence, whether oral or in writing, the probative value of which depends upon the credibility of any person other than the person giving such evidence

The above definition of hearsay applies to both civil and criminal matters.[51] Interestingly, as noted by Schwikkard and Van der Merwe[52] (referring also to Zeffert, Paizes and Skeen)[53] there may be some debate insofar as the interpretation of the word "depends" in the definition above is concerned. The nuance or issue of interpretation is this: when applying the above definition (to any form of evidence, electronic included), does the word "depends" mean that the probative value of the evidence depends entirely on another person? Or only partially? In my view, the answer lies somewhere between the two.[54]

As suggested by Zeffert and Paizes,[55] the preferred interpretation must be that the probative value of the evidence depends substantially, primarily or sufficiently upon the credibility of any person other than the person giving evidence. An analysis of hearsay-related cases decided before the *Law of Evidence Amendment Act* was promulgated, going back as far as 1837,

51 Hofman and De Jager "South Africa" 770.

52 Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 275 (particularly para 13.4); Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 293-294.

53 Zeffertt, Paizes and Skeen *South African Law of Evidence* 364-402; also see the newer version of this text, Zeffertt and Paizes *South African Law of Evidence* 389-391.

54 A view endorsed in Zeffertt and Paizes *South African Law of Evidence* 390-391, where the authors state: "a case may be made for reading the words as meaning depends substantially or primarily upon".

55 Zeffertt and Paizes *South African Law of Evidence* 390-391; Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 293-294.

informs the above view.[56] Be that as it may, the statutory definition of hearsay above will be the point of departure[57] when determining whether a data message constitutes hearsay evidence.

5 Can electronic evidence constitute hearsay?

It would seem at first blush that if electronic evidence were to be exempt from the rules regulating hearsay, the net effect of this approach would be to favour electronic evidence over other forms of evidence. This could lead to forum or format shopping[58] and would undoubtedly abolish any form of functional equivalence.[59] Ideally, any form of electronic evidence must be treated the same as traditional evidence – the functional equivalent as far as possible.

In terms of an approach that is consistent with functional equivalence, the United Nations[60] states that it is:

> … based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques.

At its core, a functional equivalent approach seeks to provide or facilitate an electronic equivalent for written, signed and original documents.[61] Put differently, functional equivalence is:

> … an examination of the function fulfilled by traditional form requirements and a determination as to how the same function could be transposed, reproduced, or imitated in a dematerialized environment.[62]

The *ECT Act* facilitates this approach in South Africa[63] by recognising data messages as the functional equivalent of paper.[64] A functional equivalent approach has been endorsed by South Africa's judiciary.[65]

---

56 Zeffertt and Paizes *South African Law of Evidence* 390, in particular notes 24-28 thereof where *inter alia*, *Wright v Doe Tatha (*1837) 7 AD & E 313, *R v Teper* [1952] AC 480, *S v Van Niekerk* 1964 1 SA 729 (C) and other cases are discussed.

57 *S v Ndiki* 2007 2 All SA 185 (Ck) para 31.

58 Hofman and De Jager "South Africa" 766.

59 Hofman 2006 *SACJ* 257.

60 UN 1996 http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf para 16.

61 SALRC *Discussion Paper 131* 57; Hofman 2006 *SACJ* 260.

62 Faria 2004 *SA Merc LJ* 531.

63 Theophilopoulos 2015 *TSAR* 465.

64 Mupangavanhu 2016 *SALJ* 859; Snail 2008 *JILT* 4.

65 *S v Miller* 2016 1 SACR 251 (WCC) para 52; *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd*

Prior to the promulgation of the *ECT Act*, some early decisions[66] favoured a position which suggested that electronic evidence could not constitute hearsay as it was produced by a machine, and therefore its probative value did not depend on a person.

In *Narlis v South African Bank of Athens (Narlis)*,[67] the key finding was that, for the purposes of the legislation governing the legal position at the time: "a computer, perhaps fortunately, is not a person". This decision provided the grounding for several other decisions with the result that, often, computer-based evidence was not admissible under the then applicable statutory provisions.[68]

In *S v Harper*,[69] the court considered whether a computer could be classified as a document in terms of the *Criminal Procedure Act*. It ultimately found that a computer could not be a document, and held that:

> Computers do record and store information but they do a great deal else; inter alia, they sort and collate information and make adjustments… The extended definition of 'document' is clearly not wide enough to cover a computer, at any rate where the operations carried out by it are more than the mere storage or recording of information.[70]

However, the court did note that a print-out by a computer could be a document for the purposes of the *Criminal Procedure Act*, and held that:

> It seems to me, therefore, that it is correct to interpret the word 'document' in its ordinary grammatical sense, and that once one does so the computer print-outs themselves are admissible.[71]

As noted by the court in *Ndiki*,[72] the *Harper* judgment has been misunderstood to some extent. The ratio above, as the law was then, was authority for the proposition that evidence on a computer (on computer

---

v LA Consortium & Vending CC t/a La Enterprises 2011 4 SA 577 (GSJ) para 12-13*; Ndlovu v Minister of Correctional Services* 2006 4 All SA 165; also see the court's analysis in one of the seminal cases involving electronic evidence, *S v Ndiki* 2007 2 A ll 185 (Ck), where although the term is not specifically used, the analysis performed by the court (see para 53) uses similar logic; SALRC *Discussion Paper 131* 62; Hofman and De Jager "South Africa" para 764; Hofman 2006 *SACJ* 257.

66 Mapoma *Critical Study of the Authentication Requirements* 20-26 for a perspective on the legal position governing electronic evidence in the 1990s.

67 *Narlis v South African Bank of Athens* 1976 2 SA 573 (A); Van der Merwe *et al Information and Communications Technology Law* 111; Watney 2009 *JILT* 3-4.

68 Takombe 2014 *De Rebus* 34.

69 *S v Harper* 1981 1 SA 88 (D).

70 *S v Harper* 1981 1 SA 88 (D) 259.

71 *S v Harper* 1981 1 SA 88 (D) 259.

72 *S v Ndiki* 2007 2 All SA 185 (Ck) paras 16-18, where Van Zyl J clearly and logically summarises the *S v Harper* judgment.

storage) would not be covered by the exception in the *Criminal Procedure Act*. However, if the information were reduced to a print-out, the evidence (as long as it met the statutory requirements in the *Criminal Procedure Act*) could be regarded as a document, and therefore admissible.

Moreover, in *Ex Parte Rosch*[73] the court ultimately found that the *Law of Evidence Amendment Act* was not applicable to computer printouts because, on a basis similar to the rationale in *Narlis*, the court found that a computer was not a person. It held that:

> The provisions of the Law of Evidence Amendment Act regarding hearsay evidence were not applicable as the computer was not a 'person'.[74]

Further, in *S v Mashiyi,*[75] another case based on the rationale of the *Narlis* matter, the court found that it was unable in terms of the prevailing law at the time to admit documents which contained information that had been processed and generated by a computer.[76] It reached this decision on the grounds that a computer is not a person, and therefore evidence produced by a computer could not depend on the probative value of a person. This authority, although of little consequence today (decided pre the *ECT Act*), is doubtful.[77]

In *Ndiki*[78] the court rejected the reasoning above and stated as follows:

> Cutting away the frills, the suggested approach, based on the aforegoing decisions [*Narlis, Ex Parte Rosch* and *Mashiyi*], is that a computer is not a person and if it carried out active functions, over and above the mere storage of information, the disputed documents are inadmissible. For the same reason the Law of Evidence Amendment Act relating to hearsay evidence is also of no assistance because hearsay evidence only extends to oral or written statements, the probative value of which depends upon the credibility of a "person". As I would indicate hereinunder*, such an approach to computer generated evidence is in my view incorrect and of very little assistance.* (My emphasis).

---

73 *Ex parte Rosch* 1998 1 All SA 319 (W).
74 *Ex parte Rosch* 1998 1 All SA 319 (W) 321.
75 *S v Mashiyi* 2002 2 SACR 387 (Tk).
76 *S v Mashiyi* 2002 2 SACR 387 (Tk) 390-391.
77 Zeffertt and Paizes *South African Law of Evidence* 432, particularly fn 313; De Villiers (1) 2010 *TSAR* 563, where the author notes he cannot support the finding in *Mashiyi* and criticizes the judgment on the basis that the common law of evidence was overlooked, and states as follows: "Where there was or is no provision in legislation, or where the documents do not comply with statutory requirements, the common law of evidence could still have been used in order to get documents (also in the form of computer print-outs) admitted."
78 *S v Ndiki* 2007 2 All SA 185 (Ck) paras 11-12.

A misunderstanding[79] of technology, and the nature of a computer and its applications most likely led to these early approaches. The primary position adopted by Van Zyl J in *Ndiki* (and his rejection of the logic above) should be endorsed and followed in subsequent decisions. It is a pragmatic and common sense approach which also aligns itself with international best practice.[80]

As noted elsewhere,[81] the view that a computer is not a person (and therefore that its probative value does not depend on a person) misses the point that at some stage in its genesis all computers (and data messages) rely on the credibility of some person to design[82], activate,[83] programme, enable, disable etcetera the computer or automated system. Moreover, this view arguably doesn't take account of South Africa's position on evidence in general – that is, the distinction between real and documentary evidence, where an object should be admissible in any event (subject to its being relevant).

The *Law of Evidence Amendment Act* notwithstanding, section 15 of the *ECT Act* provides for the admissibility of electronic evidence. This section has had a "huge impact"[84] on evidence. Section 15 (1) reads as follows:

> 15. Admissibility and evidential weight of data messages
>
> (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence-
>
> (a) on the mere grounds that it is constituted by a data message; or
>
> (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

Early academic views[85] on this section favoured an interpretation[86] that would exempt electronic evidence from the rules regulating hearsay

79 Fourie *Using Social Media as Evidence* 31.

80 Van der Merwe *et al Information and Communications Technology Law* 130, where the authors praise the Judgment in *Ndiki*. See Swales 2018 *PELJ* 9-17 for an analysis of the situation in selected foreign jurisdictions.

81 Zeffertt and Paizes *South African Law of Evidence* 433.

82 Fourie *Using Social Media as Evidence* 31-32.

83 SALRC *Discussion Paper 131* 68-69.

84 De Villiers (2) 2010 *TSAR* 731.

85 Collier 2005 *JBL* 6; Hofman 2006 *SACJ* 262.

86 Collier 2005 *JBL* 6; although this interpretation appears to have been retracted by Collier herself in Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 414-415, particularly fn 42-43 thereof. The chapter dealing with electronic evidence in the latest version of this text, Schwikkard and Van der Merwe *Principles of Evidence* 4th ed, is written by a different author and this early view is not canvassed in any detail.

altogether, with a court being primarily focused on assessing the weight[87] of the electronic evidence and simply admitting all forms of electronic evidence. Both the courts and other academics have rejected[88] this position.

Consequently, since this early debate on the import and meaning of section 15 of the *ECT Act*, there is acceptance[89] that data messages are not exempt from the rules regulating hearsay.

In *Ndlovu* the court held that "there is no reason to suppose that section 15 seeks to override the normal rules applying to hearsay evidence."[90] It further noted that the "the rules relating to hearsay evidence have not been excluded entirely by section 15(1)."[91] Finally, the court expressed the opinion that if a data message were to be rendered admissible in all circumstances "without further ado", then that position would clearly "elevate"[92] data messages above traditional forms of evidence.

In support of *Ndlovu*, Bozalek J in *S v Brown*[93] (*Brown)* held:

> I agree with the observation of Gautschi AJ [in *Ndlovu*] that sec 15(1)(a) does not render a data message admissible without further ado. The provisions of sec 15 certainly do not exclude our common law of evidence.

Furthermore, in *Ndiki*[94] the court held:

> The definition of hearsay quite clearly extends to documentary evidence. Whether or not the evidence contained in the document can be said to depend upon the credibility of a person, is a factual question that must in turn be determined from the facts and circumstances of each case… where the

87 Bellengere *et al Law of Evidence* 76.

88 *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 16; *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 172; *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a La Enterprises* 2011 4 SA 577 (GSJ) para 19; Theophilopoulos 2015 *TSAR* 474-775; Watney 2009 *JILT* para 3.1.4; Pistorius 2002 *SA Merc LJ* 737-738.

89 *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a LA Enterprises* 2011 4 SA 577 (GSJ) para 19; Hofman 2006 *SACJ* 262; Theophilopoulos 2015 *TSAR* 474-475; *S v Ndiki* 2007 2 All SA 185 (Ck) para 31; Zeffertt and Paizes *South African Law of Evidence* 432-435; Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 441-446.

90 *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 172-173.

91 *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 172-173; Hofman and De Jager "South Africa" 767-768.

92 *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 173.

93 *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 18.

94 *S v Ndiki* 2007 2 All SA 185 (Ck) para 31.

> probative value of a statement in the print-out is dependent upon the "credibility" of the computer itself, section 3 will not apply.

Moreover, in *LA Consortium*[95] the court held:

> The principle of 'functional equivalence' does not free data messages from the normal structures of the law of evidence...

In summation: can a data message constitute hearsay within the meaning of the *Law of Evidence Amendment Act*? In short, yes. Simply put, section 15 of the *ECT Act* does not override the normal rules applying to hearsay insofar as data messages are concerned.[96] Moreover, the *ECT Act* ensures that data messages are functional equivalents of paper.[97] Consequently, except where specific exceptions are made, then the normal common law pertaining to hearsay and admissibility applies equally to documentary hearsay as it does to electronic hearsay.[98]

Finally, the provisions of section 15 of the *ECT Act* do not free data messages from the exclusionary hearsay rules – if the credibility of the data message depends upon a natural person. Conversely, if a data message's credibility depends substantially upon a computer,[99] (for example, GPS data or mobile phone call records) then that evidence should be regarded as real[100] in nature and should not be subject to a hearsay enquiry.[101]

---

95 *La Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a LA Enterprises* 2011 4 SA 577 (GSJ) para 13.

96 *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 18; *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 172-173; *S v Ndiki* 2007 2 All SA 185 (Ck) para 31; *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a LA Enterprises* 2011 4 SA 577 (GSJ) para 13; Theophilopoulos 2015 *TSAR* 474-475; Watney 2009 *JILT* 8-9; Hofman and De Jager "South Africa" 776-777; Zeffertt and Paizes *South African Law of Evidence* 432-435; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 415.

97 Papadopoulos and Snail *Cyberlaw@SA III* 322.

98 Van der Merwe *et al Information and Communications Technology Law* 130; Hofman and De Jager "South Africa" 766.

99 Theophilopoulos 2015 *TSAR* 474, in particular fn 31.

100 Lochner, Benson and Horne 2012 *Acta Criminologica* 77.

101 *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 171-173; *S v Ndiki* 2007 2 All SA 185 (Ck) para 31; *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a La Enterprises* 2011 4 SA 577 (GSJ) para 13.

6 How does one consistently determine whether a data message is documentary evidence or real evidence?

Real evidence[102] consists of objects (things) – tangible items – that are in and of themselves evidence, and are available for inspection by the court – for example, a gun, a bullet or a knife.[103] As noted in *S v M*:[104]

> Real evidence is an object which, upon proper identification, becomes, of itself, evidence (such as a knife, photograph, voice recording, letter or even the appearance of a witness in the witness-box).

Real evidence[105] is not subject to exclusion[106] if relevant (and if no other statutory exception excludes it)[107] and it is not subject to the hearsay rules[108] for the simple reason that it is what it purports to be. However, real evidence (traditionally, in any event) is typically meaningful only when supplemented by witness testimony – ie: someone who explains its relevance.[109]

Consequently, as real evidence a data message would not need to be admitted to court under one of the various hearsay exceptions,[110] and technically is evidence in and of itself to which a court must accord appropriate weight (even without oral testimony – although, without oral testimony the evidence is likely to have little evidentiary weight). Therefore, if evidence is real in nature, it is not conceptually correct to subject that evidence to a hearsay enquiry.

In terms of documentary evidence, and the narrow *Civil Proceedings Evidence Act*[111]*(CPEA)* definition of document notwithstanding, our courts

---

102 Mason and Seng "Real Evidence" 39 define real evidence as "material objects other than documents, produced for inspection of the court" relying on Malek *Phipson on Evidence* paras 1-14. Also see Mason and Seng "Real Evidence" 36-69.

103 Zeffertt and Paizes *South African Law of Evidence* 849; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 395-396; Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 421.

104 *S v M* 2002 2 SACR 411 (SCA) para 31.

105 SALRC *Discussion Paper 131* 35-37.

106 Hofman 2006 *SACJ* 268.

107 Hofman and De Jager "South Africa" 776.

108 Hofman and De Jager "South Africa" 776; *S v Ndiki* 2007 2 All SA 185 (Ck) para 31; *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 173.

109 Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 395; Zeffertt and Paizes *South African Law of Evidence* 849; Hofman and De Jager "South Africa" 776-779; Van der Merwe *et al Information and Communications Technology Law* 124-130.

110 Swales 2018 *PELJ* 2-9; see also Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 310-323.

111 *Civil Proceedings Evidence Act* 25 of 1965 (the CPEA).

have taken differing views on the meaning of the word document[112] and have grappled with how best to classify electronic types of evidence.[113]

This inconsistency in approach is particularly problematic in the context of electronic evidence where the classification of evidence (ie: real or documentary) is an important consideration[114] in determining the evidentiary rules applicable. For example, in the case of *Seccombe v Attorney-General*[115] it was held that the word document is:

> a very wide term and includes everything that contains the written or pictorial proof of something. It does not matter of what material it is made…[116]

This definition suggests that a data message could be included in the definition of document.[117] Conversely, however, in *S v Mpumlo*[118] the court found that video evidence is not a docume*n*t, and classified the evidence as real evidence[119] by finding that:

> I have no doubt that a video film, like a tape recording, is real evidence, as distinct from documentary evidence, and, provided it is relevant, it may be produced as admissible evidence, subject of course to any dispute that may arise either as to its authenticity or the interpretation thereof.[120]

On the logic followed by the court in *Mpumlo*, data messages can also be treated as real evidence. The court must, however, be satisfied regarding the relevance of the evidence, and its admissibility will be subject to any dispute regarding authenticity.

In *S v Baleka (1)*[121] the court agreed with the approach in *Mpumlo* above, but only insofar as the video aspect of the evidence is concerned (leaving

---

112 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 313-315.

113 *S v Ndiki* 2007 2 All SA 185 (Ck); *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a La Enterprises* 2011 4 SA 577 (GSJ); *Ex parte Rosch* 1998 1 All SA 319 (W); *S v Mashiyi* 2002 2 SACR 387 (Tk); *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W); *S v Brown* 2015 ZAWCHC 128 (17 August 2015).

114 Fourie *Using Social Media as Evidence* 8-16.

115 *Seccombe v Attorney-General* 1919 TPD 270.

116 *Seccombe v Attorney-General* 1919 TPD 270 277; *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 19; Hofman 2006 *SACJ* 268.

117 De Villiers (1) 2010 *TSAR* 564-572.

118 *S v Mpumlo* 1986 4 All SA 197 (E); Fourie *Using Social Media as Evidence* 8-16; Van Tonder *The Admissibility and Evidential Weight of Electronic Evidence* paras 16-18.

119 Zeffertt and Paizes *South African Law of Evidence* 854 where this decision is criticised.

120 *S v Mpumlo* 1986 4 All SA 197 (E) 202.

121 *S v Baleka (1)* 1986 4 SA 192 (T).

the categorisation and question of the audio aspect open). Van Dijkhorst J[122] held as follows:

> I agree with the conclusion of Mullins J (in *Mpumlo*) that a video tape is real evidence.

However, in *S v Ramgobin*[123] the court took the opposite view to *Mpumlo* and found that video evidence is indeed documentary. This view guards against the possibility of doctored or edited evidence's being admissible. There is strong support for this decision by the widely quoted academic author Zeffert.[124]

In *S v Baleka (3)*[125] the court had occasion to consider *Ramgobin*, and rejected this approach and stated:

> I deal with tape recordings as I would deal with any other type of real evidence tendered where its admissibility is disputed. The test is whether it is relevant. It will be relevant if it has probative value. It will only have probative value if it is linked to the issues to be decided.[126]

Importantly, in *S v Nieuwoudt*[127] and S v *Fuhri,*[128] two appeal matters, it was held that the approach in *Baleka* (3) was preferable.

Insofar as technology is concerned, one may ask: how can these decisions be interpreted in the context of data messages? On the one hand, the only hurdle to admissibility is relevance (if the data message is classified as real evidence); but on the other, in addition to relevance the data message must also be an accurate representation of the information.

Based on the logic in *Baleka* (3), and those cases that support it, the classification of a data message as real evidence will mean that if a court determines that the data message is relevant, the evidence is admissible. On this logic and rationale, the enquiry about authenticity and accuracy will be central when a court accords the evidence weight, rather than when a court considers its admissibility.

However, in *S v Koralev*,[129] a child pornography matter involving data messages in the form of digital photographs, the court noted, "because of

122 *S v Baleka (1)* 1986 4 SA 192 (T) 433.
123 *S v Ramgobin* 1986 4 SA 117 (N).
124 Zeffertt and Paizes *South African Law of Evidence* 855-857.
125 *S v Baleka (3)* 1986 4 SA 1005 (T).
126 *S v Baleka (3)* 1986 4 SA 1005 (T) 1026.
127 *S v Nieuwoudt* 1990 4 SA 217 (A).
128 *S v Fuhri* 1994 2 SACR 829 (A) 835.
129 *S v Koraley* 2006 2 SACR 298 (N).

modern technology, it is essential for evidence in relation to such images to be approached with extreme caution."[130] The court endorsed the approach in *Baleka* (3), but in effect what it did was introduce a modified version of the rationale in *Ramgobin*[131] by finding that in order for it to be admissible, real evidence must not only be relevant but also accurate (with some form of corroboration as to the accuracy of the image). The court held:

> Before the images in question could be admissible in evidence against the appellants there had to be some proof of their accuracy in the form of corroboration that the events depicted therein actually occurred.[132]

Consequently, before the digital images could be admissible, the court found that there had to be some proof of their accuracy in the form of corroboration – for example, a photographer or some other witness would have to testify as to the veracity of the images.

As noted by Hofman,[133] it is possible to adopt the interpretation taken in these video and audio admissibility cases to data messages. Therefore, if one prefers the approach in the KwaZulu-Natal cases[134] illustrated by *Ramgobin*, and to an extent by *Koralev*, then a data message that relies on the credibility of a computer would be admissible if it is relevant **and authentic**.

Conversely, if one prefers the approaches taken in the Gauteng cases via *Baleka (1)* and *Baleka (3)* (and supported by Hefer JA in the two appeal decisions), then authenticity is not a pre-requisite for admissibility, and a data message that relies substantially on the credibility of a computer will be admissible if relevant.[135]

Consequently, there is a strong argument in the context of data messages that where the credibility of the data message substantially depends on the credibility of a computer, application, machine or mechanical process, it is real evidence and needs only to be relevant to be admissible. Conversely, there is an equally strong argument to suggest that the data message must not only be relevant to be admissible, but must also be accurate (authentic).

---

130 *S v Koraley* 2006 2 SACR 298 (N) 307.

131 Zeffertt and Paizes *South African Law of Evidence* 852, where the authors also reach this conclusion.

132 *S v Koraley* 2006 2 SACR 298 (N) 306-307.

133 Hofman and De Jager "South Africa" 777-779.

134 Also see *S v Singh* 1975 1 SA 330 (N).

135 *Motata v Nair 2009 1 SACR 263 (T)* para 21, where the court summarises the various approaches.

In *Motata v Nair*[136] the court weighed up the various approaches and held it was unnecessary to decide whether proof of authenticity is in fact a prerequisite for the admissibility of audio recordings. Consequently, the issue that is unclear is as follows: in order for a data message (which is real evidence) to be admissible, must it be accurate (authentic)? Alternatively, only relevant?

Given the ease of manipulation[137] of data messages, the production of some evidence to show the court that the data message is authentic (an accurate and reliable representation of the information) is probably desirable, but quite what that evidence is in each case will turn on the relevant facts and be at the discretion of each judicial officer.

Authenticity as a pre-requisite for admissibility (in addition to relevance) is supported by: *Koralev* (which dealt specifically with data messages); widely quoted academics;[138] *Ramgobin*; and is consistent with the most recent High Court judgment of *LA Consortium*[139] (the Supreme Court of Appeal has not yet had occasion to consider this issue).

Conversely, there appears to be equal justification for a court to accept data messages as evidence on the basis that they are relevant (when the evidence is real[140] in nature) – and then to consider accuracy when determining weight. Indeed, it will be interesting to see which approach South Africa's decisive courts elect to take when (not if) this issue reaches the Supreme Court of Appeal.

The above judicial debate notwithstanding, there is an argument that video, audio and graphics more closely resemble documentary rather than real evidence. Hofman[141] states:

---

136 *Motata v Nair 2009 1 SACR 263 (T)* para 21.

137 Theophilopoulos 2015 *TSAR* 461; Zeffertt and Paizes *South African Law of Evidence* 852-854.

138 Zeffertt and Paizes *South African Law of Evidence* 852.

139 *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a LA Enterprises* 2011 4 SA 577 (GSJ) paras 12-13, where the court found that the evidence was both real and documentary. In so doing it applied a hearsay enquiry to admit the evidence and considered the authenticity and reliability of the evidence as key factors to be considered before admitting the evidence.

140 SALRC *Discussion Paper 131* 35-36, where English barrister and author Mason states: "emerging jurisprudence, globally, seems to suggest that computer printouts may constitute real evidence".

141 Hofman 2006 *SACJ* 268; *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 19; Hofman and De Jager "South Africa" 778.

> video, audio and graphics now resemble documents more than the knife and bullet that are the traditional examples of real evidence

Accordingly, some authors are of the view that graphics, audio and video in data message form should be classified as documentary evidence.[142] This view was accepted by the Western Cape High Court in *Brown,*[143] where the court had occasion to discuss how best to classify evidence as real or documentary. The decision in *Ndiki*[144] was endorsed and the court found that the best approach is to consider the nature[145] of the evidence, together with the reason for its admission. Furthermore, the court in *Brown* found that much like in *Ndiki* the transient and fluid nature of electronic communications meant that its admission into evidence is better suited as a document rather than as an object (real evidence).[146]

With that being the case, in circumstances where it is not considered real in nature, in order to admissible[147] an electronic communication in the form of a document must be: produced, original and authentic (subject to concessions provided in the *ECT Act* regarding originality and production).[148]

As noted by Gautschi AJ:[149]

> For documentary evidence to be admissible, the statements contained in the document must be relevant and otherwise admissible; the authenticity of the document must be proved; and the original document must normally be produced.

Therefore, the question of whether a data message is a document (documentary evidence) or an object (real evidence) can be pivotal in determining whether evidence is admissible or inadmissible (due to hearsay), and will further dictate the hurdles to be overcome in its reception to court. This issue can be controversial,[150] and arguably requires law

142 Hofman 2006 *SACJ* 268; Zeffertt and Paizes *South African Law of Evidence* 852.
143 *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 18.
144 *S v Ndiki* 2007 2 All SA 185 (Ck) para 53.
145 *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 20.
146 *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 20.
147 Theophilopoulos 2015 *TSAR* 461-480.
148 Theophilopoulos 2015 *TSAR* 461-480; Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 431-435.
149 *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 165-166.
150 Zeffertt and Paizes *South African Law of Evidence* 432-433, where the authors disagree with the proposition that a computer can produce real evidence and rely on Bilchitz "Law of Evidence" 796 to support their position. In my view, although understandable, this position is not consistent with modern international practice and does not accord with the South African common law in relation to real evidence. As a result, the proposition that computers cannot produce real evidence should be

reform[151] - the SALRC have stated that it supports a distinction between documentary and real evidence (in the context of data messages).[152]

In *Ndlovu,* Gautschi AJ found that data messages could be either real evidence or documentary evidence, depending on the nature of the evidence, by holding as follows:

> where the probative value of the evidence depends upon the 'credibility' of the computer… section 3 of the Law of Evidence Amendment Act 45 of 1988 will not apply[153]

In *Ndiki*[154] the court followed logic similar to that in *Ndlovu* by finding that a data message will be considered real evidence if its credibility depends on the reliability of a computer, by holding that:

> Evidence on the other hand that depends solely upon the reliability and accuracy of the computer itself and its operating systems or programmes, constitutes real evidence.

However, the court in *Ndiki* did express reservations about the reliability of computer-based evidence and *obiter* expressed the view[155] that all computer-based evidence should be hearsay.[156] However, the court did not deem it necessary to finally determine this issue and left the question open.

In *LA Consortium* Malan J supported the distinction created in both *Ndlovu* and *Ndiki* by finding that evidence in the form of computer printouts was real evidence by stating that: "this is real evidence the probative value of which

---

rejected as appears to have been done with most recent case law in South Africa dealing with the issue; for example, *S v Ndiki* 2007 2 All SA 185 (Ck); *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 173; *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a LA Enterprises* 2011 4 SA 577 (GSJ).

151 SALRC *Discussion Paper 131* 68-70.

152 SALRC *Discussion Paper 131* 85, where the SALRC notes that it "supports the maintenance of a distinction between automated data messages and data messages made by a person" and proposes statutory reform.

153 *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 173.

154 *S v Ndiki* 2007 2 All SA 185 (Ck) para 7.

155 *S v Ndiki* 2007 2 All SA 185 (Ck) para 33; Hofman and De Jager "South Africa" 777, where the reservations expressed in *Ndiki* are based on the misgivings noted in the annual survey of South African law by Bilchitz – Bilchitz "Law of Evidence" – where the view espoused is that all computer-based evidence is subject to the credibility of a natural person and should therefore be regarded as hearsay. This view should be rejected as it is inconsistent with recent case law, and with South Africa's common law on real evidence.

156 This view is only *obiter dictum*, and Van Zyl J did not feel it necessary to decide this point.

depends on the reliability and accuracy of the computer and its operating systems."[157]

The court went further, unfortunately, as noted elsewhere,[158] to state that: "the data messages relied upon in this case are not only real evidence but includes hearsay." Perhaps the court meant to say there was both real evidence and documentary hearsay evidence (as was the case in *Ndiki*). The court appears to note that the probative value of the evidence depends on a computer, and is therefore real in nature,[159] however the court ultimately concludes that the evidence is hearsay in nature (but does allow it as admissible via statutory hearsay exceptions). Arguably, this classification is problematic as conceptually, real evidence cannot be subjected to a hearsay analysis. If the evidence is real in nature, it is what it purports to be.

In *Brown* Bozalek J took a conservative approach (although the court did endorse the decision in *Ndiki*), and found that even though the admissibility of photographs (stored via electronic means) were more akin to being real evidence, they were ultimately classified as documentary evidence. The court found that:

> Given the potential mutability and transient nature of images such as the images … I consider that they are more appropriately dealt with as documentary evidence rather than '*real evidence.*'[160]

Herein lies some of the controversy (or room for law reform). When should data messages be considered documentary evidence and when should they be considered real evidence? Finally, and to add a further nuance, is it possible for electronic evidence to be both real and documentary at the same time or, at the very least, exhibit characteristics of both real and documentary evidence?

---

157 *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a LA Enterprises* 2011 4 SA 577 (GSJ) para 16.

158 *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v La Consortium & Vending CC t/a LA Enterprises* 2011 4 SA 577 (GSJ) para 12; De Villiers (2) 2010 *TSAR* 733.

159 *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a LA Enterprises* 2011 4 SA 577 (GSJ) para 16.

160 *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 20.

In my view the solution is a relatively simple[161] one: consider the nature[162] of the data message, and determine whether it relies on the credibility of a person or a machine.[163] As noted in *Ndiki*:

> It is an issue that must be determined on the facts of each case having regard to what it is that the party concerned wishes to prove … the contents thereof, …the function performed by the computer and the requirements of the relevant section relied upon for the admission of the document in question.[164]

It may be that a data message exhibits characteristics of both real and documentary evidence. This was the case in both *Ndiki* and *LA Consortium*, and in these cases the evidence that is classified as real should be treated as traditional forms of real evidence. Similarly, if the evidence is documentary in nature, it should be treated in that manner (and subject to hearsay considerations).

Clearly, the distinction between whether a data message is real or documentary can be difficult to draw at times, but the apparent difficulty notwithstanding, that should not result in all data messages being treated as documentary evidence. This approach would be short-sighted and conceptually incorrect, and would ignore our common law. If the data message relies substantially on a computer or mechanical process, then that evidence should be real in nature. Equally, if a data message relies substantially on the credibility of a person, then that evidence must be treated as documentary hearsay.

7 Conclusion

Societies' increasing reliance on technology means that electronic evidence will become increasingly important. Ideally, any form of electronic evidence must be treated in the same way as traditional evidence – as the functional equivalent thereof. Accordingly, electronic evidence can certainly constitute hearsay within the meaning of the *Law of Evidence Amendment Act*. When dealing with electronic evidence, the classification thereof is critical in

---

161 De Villiers (1) 2010 *TSAR* 568-569, where the author suggests a five-step approach. In my view, this is overly complicated. A court must concern itself primarily, with the nature of the evidence and then apply the normal common law rules applicable to that type of evidence. Also see Fourie *Using Social Media as Evidence* 13-14. In my view, the nature of the evidence must primarily dictate its classification. In this regard, see *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 20; S *v Ndiki* 2007 2 All SA 185 (Ck) para 53; Theophilopoulos 2015 *TSAR* 461.

162 *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 20; S *v Ndiki* 2007 2 All SA 185 (Ck) paras 20-21.

163 S *v Ndiki* 2007 2 All SA 185 (Ck) paras 20-21; De Villiers (1) *TSAR* 2010 566-567; Fourie *Using Social Media as Evidence* 8-13.

164 S *v Ndiki* 2007 2 All SA 185 (Ck) paras 20-21.

determining whether the evidence is admissible or not (due to hearsay), and the classification will further dictate the requirements to be satisfied when admitting the evidence to court.

In order to consistently determine how to classify electronic evidence, it is imperative to consider the nature of the evidence.[165] Moreover, one must consider what role the computer or mechanised process played in the genesis of the evidence concerned. Simply put, if the credibility of the evidence depends upon a person (human thoughts or observations recorded as a data message), then this evidence should be treated as documentary hearsay. Conversely, where the evidence depends substantially upon a computer (GPS records recorded as data messages, for example), then that evidence should be classified as real evidence.

Finally, part two of this article will consider: the exceptions to the hearsay rules (applicable when electronic evidence is classified as documentary hearsay); a selected review of relevant foreign jurisdictions where South Africa may be able to learn lessons; and further law reform urgently required in relation to hearsay electronic evidence.

Bibliography

Literature

Bellengere *et al Law of Evidence*
Bellengere A *et al The Law of Evidence in South Africa* (Oxford University Press Cape Town 2013)

Bilchitz "Law of Evidence"
Bilchitz D "Law of Evidence" in Lewis C *et al* (eds) *Annual Survey of South African Law* (Juta Johannesburg 1998) 735-821

Collier 2005 *JBL*
Collier D "Evidently not so Simple: Producing Computer Print-outs in Court" 2005 *JBL* 6-9

De Villiers (1) 2010 *TSAR*
De Villiers DS "Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (part 1)" 2010 *TSAR* 558-575

165 *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 173; S *v Ndiki* 2007 2 All SA 185 (Ck) para 7.

De Villiers (2) 2010 *TSAR*
De Villiers DS "Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (part 2)" 2010 *TSAR* 720-734

Faria 2004 *SA Merc LJ*
Faria JAE "E-commerce and International Legal Harmonization: Time to Go Beyond Functional Equivalence?" 2004 *SA Merc LJ* 529-555

Fourie *Using Social Media as Evidence*
Fourie PF *Using Social Media as Evidence in South African Courts* (LLM-dissertation North-West University 2016)

Hofman 2006 *SACJ*
Hofman J "Electronic Evidence in Criminal Cases" 2006 *SACJ* 257-275

Hofman and De Jager "South Africa"
Hofman J and De Jager J "South Africa" in Mason S (ed) *Electronic Evidence* 3rd ed (LexisNexis Butterworths London 2012) 761-797

Lochner, Benson and Horne 2012 *Acta Criminologica*
Lochner H, Benson B and Horne J "Making the Invisible Visible: The Presentation of Electronic (Cell Phone) Evidence as Real Evidence in a Court of Law" 2012 *Acta Criminologica* 69-82

Malek *Phipson on Evidence*
Malek HM (ed) *Phipson on Evidence* 18th ed (Sweet & Maxwell London 2013)

Mapoma *Critical Study of the Authentication Requirements*
Mapoma SX *A Critical Study of the Authentication Requirements of Section 2 of the Computer Evidence Act No 57 of 1983* (LLM-dissertation University of South Africa 1997)

Mason and Seng "Real Evidence"
Mason S and Seng D "Real Evidence" in Mason S and Seng D (eds) *Electronic Evidence* 4th ed (Institute of Advanced Legal Studies London 2017) 36-69

Mupangavanhu 2016 *SALJ*
Mupangavanhu Y "Electronic Signatures and Non-variation Clauses in the Modern Digital World: The Case of South Africa" 2016 *SALJ* 853-873

Papadopoulos and Snail *Cyberlaw@SA III*
Papadopoulos S and Snail S (eds) *Cyberlaw@SA III: The Law of the Internet in South Africa* 3rd ed (Van Schaik Pretoria 2012)

Pistorius 2002 *SA Merc LJ*
Pistorius T "'Nobody Knows you're a Dog': The Attribution of Data Messages" 2002 *SA Merc LJ* 737-746

SALRC *Discussion Paper 131*
South African Law Reform Commission *Discussion Paper 131, Project 126 - Review of the Law of Evidence* (SALRC Pretoria 2014)

SALRC *Issue Paper 27*
South African Law Reform Commission *Issue Paper 27, Project 126 – Review of the Law of Evidence: Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (SALRC Pretoria 2010)

Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed
Schwikkard PJ and Van der Merwe SE *Principles of Evidence* 3rd ed (Juta Cape Town 2009)

Schwikkard and Van der Merwe *Principles of Evidence* 4th ed
Schwikkard PJ and Van der Merwe SE *Principles of Evidence* 4th ed (Juta Cape Town 2016)

Snail 2008 *JILT*
Snail S "Electronic Contracts in South Africa: A Comparative Analysis" 2008 *JILT* 1-24

Swales 2018 *PELJ*
Swales L "An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part Two" 2018 *PELJ* (http://dx.doi.org/10.17159/1727-3781/2018/v21i0a4496)

Takombe 2014 *De Rebus*
Takombe MO "The Rise of the Machines - Understanding Electronic Evidence" 2014 Aug *De Rebus* 32-35

Theophilopoulos 2015 *TSAR*
Theophilopoulos C "The Admissibility of Data, Data Messages, and Electronic Documents at Trial" 2015 *TSAR* 461-481

Van der Merwe *et al Information and Communications Technology Law*
Van der Merwe D *et al Information and Communications Technology Law* 2nd ed (LexisNexis Durban 2016)

Van Tonder *Admissibility and Evidential Weight of Electronic Evidence*
Van Tonder *The Admissibility and Evidential Weight of Electronic Evidence in South African Legal Proceedings: A Comparative Perspective* (LLM-dissertation University of the Western Cape 2013)

Watney 2009 *JILT*
Watney M "Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position" 2009 *JILT* 1-13

Zeffertt, Paizes and Skeen *South African Law of Evidence*
Zeffertt DT, Paizes AP and Skeen A St Q *The South African Law of Evidence, Formerly Hofman and Zeffert* (LexisNexis Butterworths Durban 2003)

Zeffertt and Paizes *South African Law of Evidence*
Zeffertt DT and Paizes AP *The South African Law of Evidence* 2nd ed (LexisNexis Durban 2009)

Case law

England

R v Teper [1952] AC 480

*Wright v Doe Tatha (*1837) 7 AD & E 313

South Africa

Delsheray Trust v ABSA Bank Limited 2014 JOL 32417 (WCC)

Ex parte Rosch 1998 1 All SA 319 (W)

Heroldt v Wills 2013 2 SA 530 (GSJ)

La Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v La Consortium & Vending CC t/a La Enterprises 2011 4 SA 577 (GSJ)

Motata v Nair 2009 1 SACR 263 (T*)*

Narlis v South African Bank of Athens 1976 2 SA 573 (A)

Ndlovu v Minister of Correctional Services 2006 4 All SA 165 (W)

R v Katz 1946 AD 71

R v Trupedo 1920 AD 58

S v Baleka (1) 1986 4 SA 192 (T)

S v Baleka (3) 1986 4 SA 1005 (T)

S v Brown 2015 ZAWCHC 128 (17 August 2015)

S v *Fuhri* 1994 2 SACR 829 (A)

S v Harper 1981 1 SA 88 (D)

S v Koraley 2006 2 SACR 298 (N)

S v M 2002 2 SACR 411 (SCA)

S v Mashiyi 2002 2 SACR 387 (Tk)

S v Miller 2016 1 SACR 251 (WCC)

S v Mpumlo 1986 4 All SA 197 (E)

S v Ndiki 2007 2 All SA 185 (Ck)

S v Nieuwoudt 1990 4 SA 217 (A)

S v Ramgobin 1986 4 SA 117 (N)

S v Singh 1975 1 SA 330 (N)

S v Van Niekerk 1964 1 SA 729 (C)

Seccombe v Attorney-General 1919 TPD 270

Legislation

Civil Proceedings Evidence Act 25 of 1965

Computer Evidence Act 57 of 1983

Constitution of the Republic of South Africa, 1996

Criminal Procedure Act 51 of 1977

Cybercrimes and Cybersecurity Bill B6-2017

Electronic Communications and Transactions Act 25 of 2002

Law of Evidence Amendment Act 45 of 1988

Government publications

Draft Cybercrimes and Cybersecurity Bill, 2015 (Gen N 878 in GG 39161 of 2 September 2015)

Draft Electronic Communications and Transactions Amendment Bill, 2012 (GN R888 in GG 35821of 26 October 2012)

International instruments

United Nations Commission on International Trade Law Model Law on Electronic Commerce (1996)

Internet sources

LSSA 2015 https://tinyurl.com/m9vght3
Law Society of South Africa 2015 *Comments to the South African Law Reform Commission in Relation to Issues Raised in Discussion Paper 131: Review of the Law of Evidence* https://tinyurl.com/m9vght3 accessed 8 December 2016

UN 1996 http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf
United Nations 1996 *Model Law on Electronic Commerce with Guide to Enactment 1996* http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf accessed 20 February 2016

UNCITRAL 2017 http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html
United Nations Commission on International Trade Law *2017: Status UNCITRAL Model Law on Electronic Commerce 1996* http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html accessed 24 February 2016

List of Abbreviations

CPEA	Civil Proceedings Evidence Act 25 of 1965
ECT Act	Electronic Communications and Transactions Act 25 of 2002
ESI	Electronically stored information
ICT	Information communication and technology
JBL	Juta Business Law
JILT	Journal of Information, Law and Technology

LSSA	Law Society of South Africa
Model Law, 1996	United Nations Commission on International Trade Law Model Law on Electronic Commerce (1996)
PELJ	Potchefstroom Electronic Law Journal
SACJ	South African Journal of Criminal Justice
SA Merc LJ	South African Mercantile Law Journal
SALJ	South African Law Journal
SALRC	South African Law Reform Commission
TSAR	Tydskrif vir die Suid-Afrikaanse Reg
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law